Spring et al. (2021) attack the Common Vulnerability Scoring System (CVSS) for a number of important features, chief among them being the lack of a formal and empirical justification. They contend that when turning qualitative data into numerical numbers, CVSS's scoring system produces inaccurate findings because it ignores the unique conditions under which vulnerabilities are exploited. Because this method focuses more on technical severity than on more complete risk aspects like human or operational context, it is less successful for firms that prioritise vulnerabilities based on actual risk rather than technical severity. The authors also draw attention to the fact that CVSS fails to take into account the material ramifications of an exploit, including potential harm to availability, confidentiality, and integrity.

I agree with this critique. Studies like Houmb et al. (2010) emphasise the need for security risk assessments that incorporate frequency, impact, and real-world consequences rather than focusing purely on technical severity. The CVSS lacks the flexibility required to address context-specific vulnerabilities and prioritise risks effectively, as also noted by Allodi and Massacci (2014), who found a disconnect between CVSS scores and exploitability.

One alternative suggested by Spring et al. is the Stakeholder-Specific Vulnerability Categorisation (SSVC), which provides a more adaptable and context-sensitive approach. SSVC allows organisations to prioritise vulnerabilities based on the specific operational environment and potential consequences, offering a more robust decision-making process compared to CVSS.

**References:**

* Houmb, S.H., Franqueira, V.N.L. and Engum, E.A., 2010. Quantifying security risk level from CVSS estimates of frequency and impact. Journal of Systems and Software, 83(9), pp.1622-1634.
* Allodi, L. and Massacci, F., 2014. Comparing vulnerability severity and exploits using case-control studies. ACM Transactions on Information and System Security (TISSEC), 17(1), pp.1-20.
* Spring, J.M., Hatleback, E., Manion, A. and Shick, A., 2021. On the inadequacy of CVSS: A systematic study. IEEE Security & Privacy, 19(2), pp.74-78.